REMARKS and ARGUMENTS

This is a Response to the Final Office Action mailed August 2, 2007.

Independent claims 90, 100, and 104 are currently amended.

Claims 93, 95, and 103 are canceled.

Claims 90–92, 94, 96–102, and 104–108 are pending.

Objections to Specification

In the Office Action mailed August 2, 2007, the Substitute Specification filed on April 26, 2007 was objected to under 35 U.S.C. 132(a) because of editing in the 2nd sentence of paragraph 0069 regarding: "Cryptoprocessor 52 may ~~should~~ be attached to the motherboard..." The word "should" expressed a preference to the preferred embodiment and not a limitation to motherboard soldering. Applicant retains the original full range of equivalents as expressed in paragraph 0110. The sentence in question has been amended to revert ~~may~~ back to should and claims 93 and 103 are now canceled. Therefore the "new matter" issue regarding claims 93 and 103 is moot.

Claim Rejections – 35 USC § 112

In the Office Action mailed August 2, 2007, claims 90 and 100 were rejected for failing to distinctly claim the invention and being indefinite for use of the phrase "substantially". Claims 90, 100, and 104 have been amended to delete the word "substantially" and therefore the issue is moot. The phrase "unique identifier" has been amended to "chip identifier" which finds support in Fig. 5, item 139 and several other drawings and paragraphs.

In the Office Action mailed August 2, 2007, claims 93 and 103 were rejected under 35 U.S.C. 112, first paragraph, as claiming subject matter not described in the specification. Claims 93, 95, and 103 were in error and were not based on paragraph 0069 or on any disclosure in the present application, either amended or not amended. Claims 93, 95, and 103 have been canceled and therefore the issue is moot.

Claim Rejections – 35 U.S.C. § 103

In the Office Action mailed August 2, 2007, independent claims 90, 100, and 104, and some claims dependent thereon, were rejected under 35 USC § 103(a) as being unpatentable over Ishibashi et al. (US 6,728,379 B1) hereinafter "Ishibashi" in view of McCarty (US 5,666,411) hereinafter "McCarty".

As stated in the recent Office Action (claim 90 element codes are here referenced), Ishibashi teaches a method of securely distributing content data for processing in a single-chip secure cryptoprocessor comprising:

(a) encrypting in a network server content data under control of an encryption key;

(b) transmitting encrypted content data to a user-side cryptoprocessor;

(e) encrypting a decryption key to produce an encrypted data block;

(f) transmitting said data block to said cryptoprocessor chip;

(g) decrypting said data block in said cryptoprocessor chip to produce a decrypted said decryption key in said cryptoprocessor chip; and

(h) decrypting said encrypted content data in said cryptoprocessor chip under control of said decryption key to produce decrypted content data.

As stated in the recent Office Action, page 6, lines 12–21 (and reflecting current amendments to claim 90), Ishibashi does not teach:

(c) encrypting a chip identifier in said cryptoprocessor chip to produce an encrypted identifier;

(d) transmitting said encrypted identifier to said server;

(e) reencrypting in said server said chip identifier together with a decryption key corresponding to said encryption key to produce an encrypted data block;

(g) decrypting said encrypted data block in said cryptoprocessor chip to produce a decrypted identifier and said decryption key in said cryptoprocessor chip;

(h) decrypting said encrypted first program in said cryptoprocessor chip under control of said decryption key to produce executable digital instructions stored in said program memory; and

(i) executing said digital instructions in said processor core in said cryptoprocessor chip to generate output data if said decrypted identifier has a predetermined relationship with said chip identifier in said cryptoprocessor chip.

Moreover, as stated in the recent Office Action, Ishibashi does not explicitly teach a program of executable instructions.

As stated in the recent Office Action page 7, McCarty teaches a method of securely distributing program of instructions for execution in a single-chip cryptoprocessor that contains chip identifier data ["device identifier" DEVID in McCarty col 7, Ln 33], encryption circuitry for encrypting said identifier, decryption circuitry for decrypting encrypted digital program instructions, writable program memory for storing decrypted instructions, and processor core for executing said decrypted instructions which are inaccessible [McCarty Col 24, Ln 23] from said secure cryptoprocessor chip from locations outside of said chip after fabrication of said chip is completed.

As stated in the recent Office Action (page 7, lines 10–21), McCarty teaches the method comprising:

(d) transmitting said chip identifier (DEVID) to said server [McCarty Col 10, L 62-66];

(f) receiving a data block in said cryptoprocessor chip;

(g) decrypting said data block in said cryptoprocessor chip to produce a decrypted key (SYSKEY) in said cryptoprocessor chip [McCarty, Col 11, Ln 60–65];

(h) decrypting said encrypted first program in said cryptoprocessor chip under control of a decryption key (SYSKEY) to produce executable digital instructions stored in said program memory [McCarty, Col 11, Ln 10–25]; and

(i) executing said digital instructions in said processor core in said cryptoprocessor chip [McCarty Col 7, Ln 50-52] to generate output data if said decrypted identifier has a predetermined relationship with said chip identifier in said cryptoprocessor chip [McCarty Col 10, Ln 62-67].

The recent Office action stated that the McCarty data block contains upgrade data comprising the DEVID – Ed(SYSKEY) which is the new system key encrypted under the Device (chip) key corresponding to a Device (chip) ID. [McCarty, Col 8, Ln 14–18]. SYSKEY is encrypted, not DEVID in McCarty Col 10, Ln 62-66.

However, the combination of Ishibashi and McCarty, does not teach, show, describe, or remotely suggest the following limitations in applicant's claim 90:

(c) encrypting said chip identifier in said cryptoprocessor chip to produce an encrypted identifier;

(e) reencrypting in said server said chip identifier together with a decryption key corresponding to said first encryption key to produce an encrypted data block; and

(g) decrypting said encrypted data block in said cryptoprocessor chip to produce a decrypted identifier and said decryption key in said cryptoprocessor chip.

In applicant's Fig. 2 [see claim 90 (c)] in cryptoprocessor chip 52, chip identifier 139 is encrypted 147 to produce an encrypted identifier 323 to transmit in encrypted form to server 120. McCarty does not suggest encryption of DEVID. To the contrary, McCarty teaches away from encryption of the DEVID (device identifier code and serial number) by suggesting that the DEVID could be be openly displayed whenever the operating system is re-booted. [McCarty, Col 13, Ln 39–43, 50–51].

In applicant's Fig. 2 [see claim 90 (e)] in server 120, chip identifier 139 and decryption key K1 are encrypted together 129 to produce encrypted data block 94 which is transmitted in encrypted form to cryptoprocessor chip 52. McCarty teaches encryption of decryption key SYSKEY as a function of DEVID [McCarty, Col 10, Ln 64], but not encrypting both together as one encrypted data block. Such reencryption of DEVID and SYSKEY together as one encrypted data block is not taught, shown, described, or remotely suggested in Ishibashi or McCarty.

In applicant's Fig. 2 [see claim 90 (g)] in said cryptoprocessor chip 52, encrypted data block 94 is block decrypted 99 under control of key K2 (98) to produce a decrypted data block that comprises decrypted chip identifier 139 and decryption key K1 (100) in said cryptoprocessor chip. Such block decryption of DEVID and SYSKEY from one encrypted data block is not taught, shown, described, or remotely suggested in Ishibashi or McCarty.

In summary, the proposed combination of Ishibashi and McCarty does not show, describe, or suggest the following limitations in applicant's claims 90, 100, or 104:

(c) encrypting said chip identifier in said cryptoprocessor chip to produce an encrypted identifier;

(e) reencrypting in said server said chip identifier together with a decryption key corresponding to said first encryption key to produce an encrypted data block; and

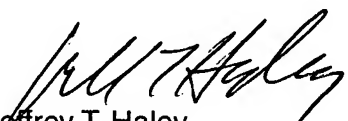
(g) decrypting said encrypted data block in said cryptoprocessor chip to produce a decrypted identifier and said decryption key in said cryptoprocessor chip.

In order to establish a *prima facie* case of obviousness, all of the claim limitations must be taught or suggested by the prior art references when combined (MPEP 706.02(j)). All of the claim limitations in claims 90, 100, and 104 were not taught or suggested. Therefore no *prima facie* case of obviousness has been established.

In view of the above, each of the presently pending claims in this application is believed to be in condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue.

Respectfully submitted,

GRAYBEAL JACKSON HALEY LLP



Jeffrey T. Haley
Registration No. 34,834
155 - 108th Avenue N.E., Suite 350
Bellevue, WA 98004-5901
(425) 455-5575.